View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Revistas Científicas de la Universidad de Cádiz

El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador

Francisco Martínez Vázquez
Diputado
Profesor de Derecho Constitucional en ICADE (Universidad de Comillas)

1. Introducción: protección de datos y garantía de derechos en la sociedad digital.

Todos los años, la *Chapman University* realiza una interesantísima encuesta acerca de los temores de los ciudadanos de Estados Unidos, que da lugar a un estudio con un título sugerente: "*America's top fears*". En las últimas ediciones, llama la atención de junto a temores perfectamente previsibles como la muerte de seres queridos o la falta de recursos para enfrentar el futuro, aparezcan entre los veinte primeros puestos el temor al tratamiento de nuestros datos personales por parte de autoridades públicas y también por corporaciones privadas. En concreto, en la edición de 2018 el puesto 17 en la escala de temores lo ocupa el "*Corporate tracking of personal data*", mientras que el puesto 18 lo ocupa el "*Government tracking of personal data*", lo que revela también otro dato interesante, como es que en su respuesta espontánea los encuestados parecen temer más a la utilización abusiva de datos personales por parte de empresas privadas que a ese mismo fenómeno realizado por organismos públicos.

En abril de 2018 Mark Zuckerberg, fundador de Facebook, hacía pública una declaración con motivo de su comparecencia ante el Congreso de Estados Unidos convocada por la millonaria fuga de datos de los usuarios de su célebre red social: "*fue un gran error, mi error, no haber tenido una visión más amplia de nuestra responsabilidad*". Uno de los fundadores de Internet, Tim Berners-Lee, afirmaba en 2011 que los datos se habían convertido en la nueva materia prima de la Tierra, lo que debe ponerse en relación con el ritmo al que se produce ese nuevo recurso de enorme valor, pues en la estimación del Foro Económico Mundial, el 90% de los datos en circulación se han generado en los 24 meses anteriores.

En este contexto, no menos impactantes son las cifras que conocemos sobre datos comprometidos o filtrados ilegalmente. Así, en la primera mitad de 2017 ya se habían filtrado más datos personales (1.900 millones) que en todo 2016 (1.370 millones) y se estima que una media de 10.4 millones de datos personales se comprometen cada día

La llamada "Cuarta Revolución Industrial", según la expresión extendida por el Foro Económico Mundial desde 2016, conlleva sus propios desafíos en campos íntimamente ligados a los derechos fundamentales y libertades públicas, que difícilmente tendrán la misma interpretación que tenían en la jurisprudencia clásica. Así, el derecho a la intimidad, la privacidad o la protección del honor, todos ellos adquieren nuevos contornos en una sociedad digital en la que el tráfico de datos alcanza magnitudes imposibles de imaginar hace solo unos años.

En este contexto, la protección de los ciudadanos frente a un uso fraudulento o abusivo de sus datos personales se ha convertido en la cuestión medular en el terreno de los derechos fundamentales y libertades públicas en el mundo digital contemporánea.

Sin embargo, no es menos cierto que en España la Constitución de 1978 tuvo algo de visionaria al contemplar hace cuatro décadas la limitación del uso de la informática en el artículo 18.4 CE, precisamente para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La inspiración del Constituyente español estuvo, probablemente, en el artículo 35 de la Constitución portuguesa de 1976, que estableció en el constitucionalismo europeo un precedente con admirable sentido anticipatorio, al incluir en la parte dogmática de la Constitución, entre los derechos fundamentales, una serie de cautelas frente al uso de la informática cuyo impacto en las libertades individuales difícilmente podía llegar a calibrarse en aquellas fechas. Este precepto tiene por rúbrica "Utilización de la informática" y establece lo siguiente:

> 1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.
>
> 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.
>
> 3. Se prohibe atribuir un número nacional único a los ciudadanos.

La previsión del artículo 18.4 CE permitió al Tribunal Constitucional construir una sólida doctrina sobre el contenido esencial de un auténtico derecho fundamental, acreedor de la más intensa protección que dispensa nuestro ordenamiento jurídico, cuyo desarrollo necesariamente correspondía al legislador orgánico.

2. El desarrollo del derecho fundamental a la protección de datos: de la LORTAD al RGPD y a la nueva LOPDP

La primera regulación de este novedoso derecho fundamental se produjo a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (conocida como LORTAD). La ratificación por España del Convenio Schengen sirvió para incorporar la protección de datos personales a un marco jurídico mucho más amplio y de indudable vocación comunitaria, tal como refleja la importante Directiva 95/46/CE, del Parlamento europeo y del Consejo, de 24 de octubre de 1995, sobre protección de datos y libre circulación de esos datos, cuya transposición al ordenamiento jurídico español se produjo mediante la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal vigente hasta hace solo unos meses.

La Carta de Derechos Fundamentales de la Unión Europea, adaptada en Estrasburgo el 12 de diciembre de 2007, recoge con claridad la protección de datos personales en el catálogo de derechos y libertades de la Unión Europea, esa especie de "contenido dogmático" de una todavía inexistente Constitución Europea. Con claridad, el artículo 8 de la Carta afirma que *"toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"*, al tiempo que impone, en su apartado segundo, que *"los datos se traten de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación"*.

La propia dinámica de la integración económica y social en la Unión Europea, así como el ritmo casi revolucionario de construcción de la sociedad digital, basada, en buena medida, en el tratamiento de flujos de datos, exigían un nuevo marco mucho más intenso y eficaz de protección del derecho reconocido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea. La disparidad normativa que permitía la Directiva comunitaria, cuya necesaria trasposición a los ordenamientos de los Estados miembros conlleva un margen de holgura que podría generar tratamientos normativos excesivamente heterogéneos, especialmente en el ámbito sancionador, hizo aconsejable apostar por el Reglamento como fuente del

Derecho comunitario reguladora de la protección de datos personales, directamente aplicable en todos los Estados miembros. Por primera vez, de forma clara, un Reglamento comunitario se convertiría en la principal norma de desarrollo de un derecho fundamental dotado de la más intensa protección constitucional.

Con esta vocación, el 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos de la Unión Europea y, con ello, un auténtico cambio de paradigma en el tratamiento de esta materia. El Reglamento es el fruto de un imprescindible y laborioso trabajo de armonización de sensibilidades, tradiciones jurídicas y procedimientos en materia de protección de datos personales en la Unión Europea, presididos por la idea de que en esta materia los esfuerzos nacionales pueden resultar estériles si no convergen hacia respuestas uniformes.

El RGPD perseguía, por tanto, el doble objetivo de evitar la fragmentación de los ordenamientos jurídicos de los Estados miembros en materia de protección de datos personales, especialmente en lo relativo al régimen sancionador y conseguir la adaptación de la normativa protectora del derecho a un entorno tecnológico completamente diferente del que vio nacer las primeras regulaciones en la materia, hasta el punto de situar la protección de datos personales en el centro mismo del debate sobre los derechos y libertades necesarios para ordenar la convivencia en la sociedad digital.

La imprescindible armonización del régimen jurídico de la protección de datos personales no consiguió, sin embargo, la pretendida uniformidad y el Reglamento Europeo (RGPD) asumió la necesidad de convivir con el respeto a ciertos ámbitos de decisión de los Estados miembros en aspectos concretos que dejaba pendientes de una posterior concreción por parte de los ordenamientos jurídicos nacionales. Es decir, el Reglamento tuvo, en ciertos aspectos, algo de la lógica normativa de la Directiva.

De conformidad con la opinión expresada por varios de los expertos que comparecieron en la Comisión de Justicia del Congreso de los Diputados para exponer su punto de vista sobre el proyecto del Ley Orgánica de Protección de Datos de Carácter Personal, el RGPD realizaba hasta 56 remisiones a la legislación de desarrollo de los Estados miembros lo que en nuestro sistema constitucional exigía la aprobación de una Ley Orgánica, por imperativo del artículo 81 CE.

Tras meses de trabajo presididos por una indudable voluntad de consenso entre las fuerzas parlamentarias y un progresivo acercamiento en los aspectos sobre los que existían discrepancias iniciales, se aprobó por unanimidad en el Pleno del Congreso y resultó aprobada sin enmiendas en el

Pleno del Senado la actualmente vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En el curso de la tramitación legislativa, el Grupo Parlamentario Socialista presentó un conjunto de enmiendas que conformaban un nuevo título en el proyecto de ley, el Título X, cuya rúbrica propuesta era "Garantía de los derechos digitales". En coherencia con tales enmiendas, la enmienda 246 del mismo grupo propuso un cambio de denominación del proyecto, que pasaría a ser Ley Orgánica de Protección de Datos Personales y de Garantía de Derechos Digitales, así como una corrección de alcance general que marcaba distancia con respecto a la Ley Orgánica 15/1999, pues la enmienda 247 proponía sustituir en todo el texto legislativo la expresión "Datos de carácter personal" por la expresión "datos personales".

La propuesta de un nuevo Título X dedicado a regular los derechos digitales desbordaba el ámbito de la iniciativa legislativa remitida por el Gobierno al Congreso de los Diputados e incluía una nueva regulación de los derechos en la sociedad digital cuya conexión con la protección de datos personales resulta en ocasiones muy tenue.

La justificación de este nuevo Título X apelaba a la necesidad de cumplir el mandato adoptado por el Congreso de los Diputados en la Proposición no de Ley para la protección de los derechos digitales aprobada el 7 de abril de 2017 y señalaba que "corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital".

Tras diferentes negociaciones entre los ponentes de los grupos parlamentarios se introdujeron importantes modificaciones con respecto al texto del proyecto y a las enmiendas iniciales, hasta quedar finalmente aprobado el texto de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El marco jurídico de la protección de datos personales, así como la primera regulación de los derechos en la sociedad digital quedaban, de este modo, recogidos en el RGPD, de aplicación directa desde el pasado 25 de mayo de 2018 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. Novedades en el ámbito de las obligaciones del responsable y el encargado

Centrándonos en las novedades que este nuevo marco jurídico introduce en la regulación de las obligaciones del responsable y el encargado, debemos comenzar por señalar que el RGPD y, por extensión, la LOPDP, se basan en la interacción de dos importantes principios: prevención y flexibilidad. La prevención se trata de alcanzar a partir de la implantación de los principios de responsabilidad y compromiso activo de quienes estén involucrados en el tratamiento de datos personales, distinguiendo las figuras del responsable y el encargado.

En el artículo 4 del RGPD, dedicado a las definiciones, se define al responsable como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento", mientras que el mismo precepto define al encargado como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

Pues bien, tanto los responsables como los encargados deben ser perfectamente conscientes del efecto que los diversos tratamientos de datos tienen sobre los titulares de los datos personales y, a partir de ese conocimiento, han de aplicar unas medidas de cumplimiento que garanticen el máximo respeto a los principios y derechos que el Reglamento y la Ley Orgánica establecen. Es lo que se denomina principio de responsabilidad activa, que se traduce en un conjunto de herramientas encaminadas a garantizar el pleno respeto a los derechos de los titulares de los datos.

El Reglamento no se conforma, por tanto, con definir unos objetivos de cumplimiento, sino que desarrolla los instrumentos necesarios para alcanzar tales objetivos y lo hace introduciendo una segunda nota, como es la flexibilidad, pues no todos los responsables y encargados están expuestos al mismo nivel de riesgo ni deben, por tanto, aplicar las mismas medidas ni hacerlo del mismo modo. Entre tales herramientas derivadas del principio de responsabilidad activa se encuentran la realización de un "registro de actividades de tratamiento", las medidas de Protección de Datos desde el Diseño, las medidas de Protección de Datos por Defecto, las Evaluaciones de Impacto, la designación de un Delegado Protección de Datos o la notificación de quiebras de seguridad.

El criterio que define el alcance de las obligaciones de proactividad de los responsables del tratamiento es, por tanto, el riesgo. Como afirma el Considerando 76 del RGPD, "la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la

naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto". El RGPD exige, por tanto, realizar un análisis sobre el riesgo que va a suponer para los derechos y libertades de los ciudadanos y para la seguridad de la información, el tratamiento de datos personales. El análisis dependerá de un conjunto de variables como los tipos de tratamiento, la naturaleza de los datos tratados, el número de interesados afectados o la variedad de tratamientos que una misma organización lleve a cabo.

La Agencia Española de Protección de Datos no solo ha desempeñado un papel fundamental en la elaboración de la LOPDP, ofreciendo un asesoramiento técnico permanente a los órganos legislativos, sino que en su función tuitiva ha publicado unas guías de enorme utilidad para hacer frente a esta exigencia de proactividad que impone el RGPD y que, naturalmente, no puede traducirse en los mismos requerimientos para responsables de un tratamiento masivo de datos que para responsables que realicen tratamientos de menor alcance y entidad. Algunas de las preguntas que formulan estas guías constituyen un check-list de enorme utilidad para la adaptación al RGPD y a la LOPDP

En cuanto a los encargados del tratamiento, la normativa anterior, bajo la inspiración de la Directiva 95/46, especificaba solo las obligaciones del responsable. Sin embargo, el RGPD contiene una expresa regulación de las obligaciones del encargado, que van más allá de su relación contractual con el responsable y que se refieren, por ejemplo, a la obligación de mantener el registro de actividades de tratamiento, determinar las medidas de seguridad aplicables o designar un Delegado de Protección de Datos en los casos previstos en el RGPD y en la LOPDP. En el artículo 28 del RGPD se imponen una serie de contenidos a la relación contractual entre el responsable y el encargado, que tratan de salvaguardar que la elección de los encargados del tratamiento ofrezca las garantías suficientes de adecuación a las exigencias del RGPD. El contrato de encargo tendrá, de este modo, un contenido mínimo que permita reducir los riesgos y cumplir fielmente con las nuevas obligaciones establecidas en la norma europea.

En RGPD prevé, asimismo, en el artículo 24 la posibilidad de adherirse a códigos de conducta o a mecanismos de certificación para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento. Se trata de herramientas potenciadas por la norma europea y ampliamente desarrolladas por la LOPD para facilitar el efectivo cumplimiento del principio de responsabilidad activa.

Como incorporación importante de la LOPDP, el artículo 39 de la misma dispone que la acreditación de las instituciones de certificación podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las Comunidades Autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

El artículo 28 LOPDP hace referencia a la ponderación del riesgo, introduciendo como herramienta la evaluación de impacto en la protección de datos e identificando en su apartado 2 determinados indicadores del mayor riesgo, como son, entre otros, que el tratamiento pudiera generar "situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados" o que "pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales".

A título indicativo, se identifican una serie de tratamientos que pueden calificarse como de alto riesgo, tales como la elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar, tratamientos a gran escala de datos sensibles u observación sistemática a gran escala de una zona de acceso público. Las autoridades de protección de datos están obligadas a confeccionar listas de tratamientos que exijan una previa evaluación de impacto e incluso de aquellos tratamientos que no lo exijan, lo que no excluye la obligación de los responsables de realizar su correspondiente análisis de riesgos y realizar la evaluación de impacto aunque se trate de tratamientos que no figuren en las listas.

En cuanto al registro de actividades de tratamiento es otra de las obligaciones fundamentales derivadas de la exigencia de proactividad, de la que solo quedan excluidas las organizaciones a las que se refiere el apartado 5 del artículo 30 del RGPD, esto es, las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales. En el registro de actividades de tratamiento se incluirá información como el nombre y datos de contacto del responsable y del Delegado de Protección de Datos si se hubiese nombrado, descripción del tratamiento y de las categorías de interesados y de datos personales tratados, transferencias internacionales de datos, etc.

Por otra parte, el tratamiento de los datos deberá limitarse, por defecto, a aquellos que sean necesarios para los fines que se pretenden. Este principio de protección de datos desde el diseño y por defecto es un claro exponente del enfoque de responsabilidad activa que preside el RGPD y se extiende a la cantidad de datos recogidos y al alcance de su tratamiento, a su plazo de conservación o a la accesibilidad a los mismos.

Especial importancia tiene también la obligación de notificación de "quiebras de seguridad" que establecen los artículos 33 y 34 del RGPD. Tales quiebras de seguridad se refieren a toda clase de incidentes y exigen que el responsable las notifique a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. La notificación debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella e incluir datos como: la naturaleza del incidente, la tipología de datos y de interesados afectados, las medidas adoptadas por el responsable para solventar la quiebra y, si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Es interesante señalar que, como consecuencia de los riesgos y desafíos inherentes a la sociedad digital, a los que nos referíamos al inicio de este trabajo, esta obligación se añade a la que impone la Directiva NIS respecto de los incidentes en el ámbito de la ciberseguridad y que ha sido incorporada a nuestro ordenamiento jurídico interno a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. De todo ello se deduce que la protección frente a incidentes que afectan a nuevas formas de agresión en la sociedad digital exige necesariamente la puesta en común de lo sucedido, como forma de prevenir y minimizar el impacto, frente a actitudes propias del pasado, que mantenían en la más absoluta reserva los incidentes de diversa naturaleza sufridos, probablemente por temor a desvelar vulnerabilidades en entornos siempre competitivos.

Finalmente, en el terreno de las obligaciones de responsables y encargados debemos hacer una específica referencia a una singularidad de la LOPDP, que no trae causa del RGPD y que, por este motivo, fue seriamente cuestionada por algunos de los ponentes en la tramitación parlamentaria del proyecto de Ley Orgánica, proponiendo incluso su eliminación a través de enmiendas de supresión que, finalmente, no fueron aprobadas. Se trata de la previsión del bloqueo de datos establecida en el artículo 32 de la LOPDP, conforme al cual "el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión". Este precepto in-

troduce una obligación adicional para los responsables del tratamiento, no prevista en el RGPD, consistente en la identificación y reserva de los datos bloqueados para impedir su tratamiento, incluyendo su visualización, salvo que se trate de poner los datos a disposición de jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento.

4. La figura del Delegado de Protección de Datos

La figura del Delegado de Protección de Datos es una de las novedades más interesantes del RGPD, a la que se refieren los artículos 37 a 39 del RGPD, completados por los artículos 34 a 37 de la LOPDP. La previsión del RGPD es que los responsables y encargados deban nombrar una persona física o jurídica como Delegado de Protección de Datos, cuando se trate de tratamientos que lleven a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala o cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales identificados en el artículo 9 del RGPD y de datos relativos a condenas e infracciones penales.

Frente a la definición amplia que realiza el artículo 37.1 del RGPD, la LOPDP trata de aportar mayor seguridad jurídica al incorporar una relación de supuestos concretos en los que es obligatoria la designación del Delegado de Protección de Datos, que se enumeran en el artículo 34 LOPDP. Se trata de una larga y heterogénea lista de supuestos que incluye desde colegios profesionales y sus consejos generales, centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas, entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala, prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio, entidades aseguradoras y reaseguradoras, empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores, entre muchas otras.

En cuanto a las condiciones que debe reunir el Delegado de Protección de Datos, el RGPD exige que "el delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conoci-

mientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39", lo que se complementa con la previsión del artículo 35 de la LOPDP que permite acreditar la cualificación exigida a través de mecanismos voluntarios de certificación "que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos". Tras la discusión parlamentaria de este precepto, la acreditación mediante mecanismos de certificación no se plantea como única forma de acreditar la cualificación para el desempeño de las funciones del Delegado de Protección de Datos.

En cumplimiento de este precepto, la Agencia Española de Protección de Datos ha aprobado un sistema de certificación de profesionales de protección de datos que facilita la evaluación de los candidatos a desempeñar el puesto y acredita que reúnen las cualificaciones profesionales y los conocimientos requeridos. Las certificaciones son otorgadas por entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación, siguiendo criterios de acreditación y certificación elaborados por la propia Agencia y los sectores afectados.

Tanto el RGPD como la LOPDP prestan especial atención a la posición del Delegado de Protección de Datos, con el fin de garantizar que pueda desempeñar su función libre de injerencias y sin someterse a instrucciones de la organización en la que presta servicio. A estos efectos, el RGPD exige que la posición del Delegado de Protección de Datos en las organizaciones garantice su total autonomía en el ejercicio de sus funciones, lo que excluye tanto la posibilidad de recibir instrucciones como la de ser sancionado o removido por el responsable o encargado, si bien la LOPD añade un importante matiz en el artículo 36, como es que la remoción o cese será posible si "incurriera en dolo o negligencia grave" en el ejercicio de sus funciones. La norma europea impone la necesidad de que el Delegado de Protección de Datos se relacione con el nivel superior de la dirección de la organización y que el responsable o el encargado le faciliten todos los recursos necesarios para el desempeño de su actividad. La dedicación no ha de ser exclusiva por lo que el RGPD le autoriza a desempeñar otras funciones en la organización, siempre que no exista conflicto de intereses.

Las funciones del Delegado de Protección de Datos se especifican en el artículo 39 del RGPD que se refiere al asesoramiento al responsable o al encargado del tratamiento y al resto del personal de la organización, respecto de las obligaciones que les incumban en materia de protección de datos; la supervisión del cumplimiento de lo dispuesto en el ordenamiento jurídico

en materia de protección de datos y de las políticas del responsable o del encargado del tratamiento, incluyendo la asignación de responsabilidades, la concienciación y la formación del personal que participa en las operaciones de tratamiento, así como las auditorías correspondientes; el asesoramiento que se le solicite acerca de la evaluación de impacto en la protección de dato y las colaboración con las autoridades de control respecto de las cuales actúa como punto de contacto para todas las cuestiones relativas al tratamiento.

Especial interés tiene la función que atribuye al Delegado de Protección de Datos el artículo 37 de la LOPDP pues hace referencia a su posible intervención en los supuestos de de reclamaciones ante las autoridades de protección de datos. Así, nuestra Ley Orgánica ofrece la posibilidad de que el afectado por un tratamiento de datos personales se dirija al Delegado de Protección de Datos antes de formalizar una reclamación contra el responsable o encargado ante la Agencia Española de Protección de Datos o ante las autoridades autonómicas de protección de datos. El Delegado deberá comunicar al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses desde que reciba la reclamación.

Asimismo, el precepto prevé que cuando se presente una reclamación ante la Agencia Española de Protección de Datos o ante las autoridades autonómicas de protección de datos sean éstas las que remitan la reclamación al Delegado de Protección de Datos, para que responda lo que proceda en el plazo de un mes. En caso de no hacerlo, continuará el procedimiento ante la autoridad de protección de datos competente.

5. El régimen sancionador

El régimen sancionador es, sin duda, uno de los contenidos del RGPD que mayor preocupación generó entre responsables y encargados tras la entrada en vigor de la norma europea. Es fácil entender el motivo si tenemos en cuenta que el artículo 83 del RGPD contempla la posibilidad de imponer multas administrativas de hasta 20.000.000 euros o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Es cierto que la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establecía ya la posibilidad de imponer sanciones administrativas de hasta 600.000 euros, lo que constituye una cuantía nada desdeñable, si bien la posibilidad de alcanzar los 20 millones de euros o el 4% del volumen de negocio anual total constituyen un salto cualitativo que generó razonable inquietud entre los sujetos especialmente concerni-

dos por la nueva normativa. No debemos olvidar tampoco que la llamativa disparidad de los ordenamientos de los Estados miembros en materia sancionadora fue, precisamente, una de las razones que llevó al legislador comunitario a desechar la elaboración de una Directiva e imponer un régimen uniforme a través de un Reglamento de aplicación directa, también en el terreno de las sanciones.

Sin perjuicio de lo anterior, el bienintencionado intento de homogeneizar el régimen sancionador en materia de protección de datos personales difícilmente podía acomodarse a las particularidades de cada Estado miembro, así como a las exigencias constitucionales en materia de infracciones y sanciones administrativas. Precisamente por esta razón, desde la perspectiva del ordenamiento español el régimen de los artículos 83 y 84 del RGPD puede resultar insuficiente desde la perspectiva de las garantías derivadas del artículo 25 CE y traducidas por la jurisprudencia constitucional en una férrea exigencia de respeto a los principios de legalidad, tipicidad, etc., hasta el punto de equiparar en este ámbito el Derecho administrativo sancionador al Derecho penal. Por esta razón, resultaba esencial la regulación del régimen sancionador en la LOPDP, lo que se produjo a través del Título IX cuya estructura y contenido se acomoda a la tradición de nuestro Derecho público en materia sancionadora y garantiza el respeto a las exigencias constitucionales, respetando, obviamente, la regulación del RGPD.

En primer término, la LOPDP identifica en el artículo 70 a los posibles infractores, que son los responsables y encargados de los tratamientos, los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta. La Ley excluye expresamente al Delegado de Protección de Datos del ámbito sancionador, sin perjuicio de que en el debate parlamentario algunas enmiendas planteaban su inclusión, si bien fueron todas rechazadas.

La segunda gran novedad que trae consigo la LOPDP es la tipificación de las infracciones en las tres categorías habituales en nuestro Derecho sancionador, esto es, infracciones muy graves, graves y leves. La técnica legislativa seguida por el legislador orgánico ha sido establecer en cada categoría la equivalencia con el precepto del RGPD, pero concretar en la mayor medida posible la descripción de la conducta tipificada como infracción. Es importante, no obstante, señalar que la clasificación de las infracciones en muy graves, graves y leves no se introduce para determinar la cuantía de las sanciones sino exclusivamente para concretar los plazos de prescripción, si bien permite una ordenación sistemática mucho más afín a nuestra tradición jurídica. La extensa descripción de las conductas típicas ha de en-

tenderse meramente ejemplificativa, si bien es evidente que proporciona mayor seguridad jurídica a los sujetos obligados.

Así, el artículo 72 de la LOPDP se remite directamente al artículo 83.5 del RGPD y seguidamente desarrolla a título no exhaustivo las conductas que pueden calificarse como vulneración sustancial de los preceptos de la norma europea, tales como el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del RGPD (principios de licitud, transparencia, etc.), el tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del RGPD, el incumplimiento de los requisitos exigidos por el artículo 7 del RGPD para la validez del consentimiento, la utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello, entre muchos otros supuestos que introducen una nota de seguridad jurídica en la genérica descripción del artículo 83 del RGPD.

Con la misma lógica jurídica, el artículo 73 de la LOPDP clarifica qué puede entenderse por vulneración sustancial de los preceptos reglamentarios previstos en el apartado 4 del artículo 83 del RGPD, a los que califica de infracciones graves. En una relación muy extensa de conductas, el precepto enumera, entre otras el tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del RGPD, no acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del RGPD; el impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, entre muchos otros supuestos.

Finalmente, el artículo 74 de la LOPDP tipifica las infracciones leves y enumera, nuevamente sin exhaustividad, un gran número de conductas que pueden entenderse como infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del RGPD. Así, entre muchas otras, el incumplimiento del principio de transparencia de la información o del derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del RGPD o no atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22

del RGPD. De este modo, la LOPDP acomoda a una estructura formal propia de nuestro Derecho sancionador el régimen de infracciones y sanciones de los artículos 83 y 84 del RGPD, proporcionando mayor seguridad jurídica y, en esa medida, una aplicación más garantista para los sujetos obligados, especialmente teniendo en cuenta que se exponen a sanciones de elevadísima cuantía, sin precedentes en otros campos de nuestro Derecho administrativo.

Con esta misma lógica, el artículo 76 complementa lo dispuesto en el RGPD con respecto a los criterios de graduación de las sanciones que prevé la norma europea, pues añade algunos criterios como son el carácter continuado de la infracción, la vinculación de la actividad del infractor con la realización de tratamientos de datos personales, los beneficios obtenidos como consecuencia de la comisión de la infracción, la posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción o la existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no pueda imputarse a la entidad absorbente, entre otros.

En última instancia, otra de las cuestiones relativas al régimen sancionador que fue objeto de discusión en la tramitación parlamentaria, habida cuenta de que el RGPD deja esta cuestión en manos de los Estados miembros, es la posibilidad de imponer sanciones económicas a las entidades públicas que infrinjan la legislación sobre protección de datos personales. Tras las correspondientes deliberaciones parlamentarias, el legislador orgánico optó por acoger el criterio de mayor tradición en nuestro Derecho público, conforme al cual las entidades enumeradas en el artículo 77.1 de la LOPDP serán objeto de sanción mediante apercibimiento. En tal categoría se encuentran los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, el Banco de España, las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las fundaciones del sector público, las Universidades públicas, los consorcios y los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

En realidad todos ellos, en tanto sean responsables del tratamiento de datos personales, quedan plenamente sujetos a la normativa que conforman el RGPD y la LOPD, si bien no pueden ser objeto de sanciones pecuniarias

sino de mero apercibimiento. En todo caso, esta posibilidad está contemplada en el apartado 1 del artículo 84 del RGPD, con arreglo al cual "los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias".

6. Conclusiones

El mundo digital en el que vivimos desde hace años impone un ritmo de adaptación mucho más exigente de lo que estábamos acostumbrados, lo que resulta especialmente relevante cuando se trata de proteger derechos fundamentales de las personas. En una economía digital que convierte el tráfico de datos en objeto de explotación comercial y aprovechamiento lucrativo, se impone reformular algunos de los derechos tradicionales y definir otros de tal forma que se adapten a las nuevas formas de agresión a los mismos. En este terreno, la protección de datos personales que desde hace años fue calificada por el Tribunal Constitucional como verdadero derecho fundamental, adquiere nuevos contornos que se traducen en derechos y obligaciones necesariamente adaptados a una sociedad global y digital.

La respuesta es una compleja norma europea, el RGPD, que por primera vez constituye el desarrollo directo de un derecho al que nuestra Constitución garantiza la máxima protección. El imprescindible complemento de la norma europea ha llegado algunos meses después de la entrada en vigor del Reglamento, mediante la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. La aplicación de ambas normas por las autoridades de protección de datos y, en última instancia, por los órganos jurisdiccionales e incluso por el Tribunal Constitucional serán el hito decisivo para evaluar si la protección del derecho en el nuevo entorno es suficientemente completa, clara y efectiva.

Normativa

LOPDP: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Boletín Oficial del Estado* nº 294, de 6 de diciembre de 2018.

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (*Reglamento General de Protección de Datos*). *Diario Oficial de la Unión Europea,* L 119/1, de 4 de mayo de 2016.

Bibliografía

COTINO HUESO, L. (2018), "La necesaria actualización de los derechos fundamentales como derechos digitales ante el desarrollo de Internet y las nuevas tecnologías", en *España Constitucional (1978-2018). Trayectorias y perspectivas*, PENDÁS GARCÍA, B. (director), Centro de Estudios Políticos y Constitucionales, Madrid, 2018.

DÍAZ DÍAZ, E. (2016), "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", *Revista Aranzadi Doctrinal*, nº 6, 2016.

RALLO LOMBARTE, A. (2012), "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político (UNED)*, n.º 85, septiembre-diciembre 2012.

RALLO LOMBARTE, A. (Director) y otros (2019), *Tratado de Protección de Datos*, Tirant lo Blanch, Valencia, 2019.

TRONCOSO REIGADA, A. (2010), *La protección de datos personales en busca del equilibrio,* Tirant lo Blanch, Valencia, 2010.